JASON R. HULL [11202]
JHULL@MOHTRIAL.COM
TREVOR C. LANG [14232]
TLANG@MOHTRIAL.COM
MARSHALL OLSON & HULL, PC
NEWHOUSE BUILDING
TEN EXCHANGE PLACE, SUITE 350
SALT LAKE CITY, UTAH 84111
TELEPHONE: 801.456.7655

SAMUEL J. STRAUSS *
SAM@TURKESRAUSS.COM
RAINA C. BORRELLI*
RAINA@TURKESTRAUSS.COM
TURKE & STRAUSS LLP
613 WILLIAMSON STREET, SUITE 201
MADISON, WI 53703
TELEPHONE: 608.237.1775
*PRO HAC VICE FORTHCOMING

ATTORNEYS FOR PLAINTIFFS AND
PROPOSED CLASS COUNSEL

IN THE UNITED STATES DISTRICT COURT

DISTRICT OF UTAH, CENTRAL DIVISION

LAZARO STERN, on behalf of himself and all others similarly situated, Plaintiff, v. ACADEMY MORTGAGE CORPORATION, Defendant.	**COMPLAINT** **[PROPOSED CLASS ACTION]** JURY TRIAL DEMANDED Case No. 2:24-cv-15

Plaintiff, Lazaro Stern ("Plaintiff"), on behalf of himself and all others similarly situated, states as follows for his class action complaint against Defendant, Academy Mortgage Corporation, ("Academy Mortgage" or "Defendant"):

INTRODUCTION

1. On March 21, 2023, Academy Mortgage, a mortgage company that touts itself to be one of the top independent purchase lenders of the Country, discovered it had lost control over its computer network and the highly sensitive personal information stored on the computer network in a data breach perpetrated by cybercriminals ("Data Breach").

2. On information and belief, the Data Breach began on or around March 21, 2023.

Following an internal investigation, Defendant learned cybercriminals had gained unauthorized access to its consumers' personally identifiable information ("PII"), including but not limited to name and Social Security number.

3. On or about December 20, 2023–an appalling nine months after the Data Breach occurred– Academy Mortgage finally began notifying Class Members about the Data Breach ("Breach Notice"). A sample of the Breach Notice is attached as Exhibit A.

4. Upon information and belief, cybercriminals were able to breach Defendant's systems because Defendant failed to adequately train its employees on cybersecurity, failed to adequately monitor its agents, contractors, vendors, and suppliers in handling and securing the PII of Plaintiff, and failed to maintain reasonable security safeguards or protocols to protect the Class's PII—rendering them easy targets for cybercriminals.

5. Defendant's Breach Notice obfuscated the nature of the breach and the threat it posted—refusing to tell its consumers how many people were impacted, how the breach happened, or why it took the Defendant nine months to finally begin notifying victims that cybercriminals had gained access to their highly private information.

6. Defendant's failure to timely report the Data Breach made the victims vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII.

7. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII misuse.

8. In failing to adequately protect its consumers' information, adequately notify them about the breach, and obfuscating the nature of the breach, Defendant violated state law and

harmed an unknown number of its current and former consumers.

9. Plaintiff and the Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class trusted Defendant with their PII. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

10. Plaintiff is a former Academy Mortgage consumer and Data Breach victim.

11. The exposure of one's PII to cybercriminals is a bell that cannot be unrung. Before the Data Breach, the private information of Plaintiff and the Class was exactly that—private. Not anymore. Now, their private information is permanently exposed and unsecure.

PARTIES

12. Plaintiff, Lazaro Stern, is a natural person and citizen of Florida, residing in Miami, Florida, where he intends to remain.

13. Defendant, Academy Mortgage, is incorporated in Utah, with its principal place of business at 339 West 13490 South Draper, Utah 84020. Defendant can be served through its registered agent, Corporation Service Company at 15 West South Temple, Suite 600 Salt Lake City, Utah 84101.

JURISDICTION & VENUE

14. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs; there are more than 100 members in the proposed class; and Plaintiff and Defendant are citizens of different states.

15. Academy Mortgage is incorporated in Utah and maintains its principal place of business in 339 West 13490 South Draper, Utah 84020. Academy Mortgage is thus a Utah citizen.

16. This Court has personal jurisdiction over Academy Mortgage because it is a citizen

in this District and maintains its headquarters and principal place of business in this District.

17. Venue is proper because Academy Mortgage maintains its headquarters and principal place of business in this District.

FACTUAL ALLEGATIONS

Academy Mortgage

18. Academy Mortgage touts itself as a "recognized and respected nationwide" for providing "exceptional service and the best solutions and tools to help individuals and families achieve successful homeownership."[1] It boasts over $35 million in annual revenue.[2]

19. On information and belief, Academy Mortgage accumulates highly private PII of its consumers.

20. In collecting and maintaining its consumers' PII, Defendant agreed it would safeguard the data in accordance with its internal policies as well as state law and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their PII.

21. As the alleged world leader in the mortgage service industry, Academy Mortgage understood the need to protect its current and former consumers' PII and prioritize its data security.

22. Despite recognizing its duty to do so, on information and belief, Academy Mortgage has not implemented reasonably cybersecurity safeguards or policies to protect employee PII or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result, Academy Mortgage leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to consumers' PII.

[1] Academy Mortgage Corporation, Linkedin, https://www.linkedin.com/company/academy-mortgage-corporation/ (last visited January 4, 2024).
[2] Academy Mortgage Corporation, Zippia, https://www.zippia.com/academy-mortgage-careers-13386/revenue/ (last visited January 4, 2024).

Mortgage Corporation Fails to Safeguard Consumers' PII

23. Plaintiff is a former consumer of Academy Mortgage.

24. As a condition of receiving mortgage services from Academy Mortgage Plaintiff provided Defendant with his PII, including but not limited to his name and Social Security number. Defendant used that PII to facilitate its mortgage services and required Plaintiff to provide that PII to obtain its mortgage services.

25. On information and belief, Academy Mortgage collects and maintains consumers' unencrypted PII in its computer systems.

26. In collecting and maintaining PII, Defendant implicitly agreed that it will safeguard the data using reasonable means according to their internal policies as well as state and federal law.

27. Indeed, Academy Mortgage promises in its privacy policy that it "values the privacy of our visitors, users, customers, applicants, and partners" assuring its consumers that it "respects your privacy and is committed to protecting it[.]"[3]

28. Academy Mortgage further claims that "[w]e will take all the steps reasonably necessary to ensure that your information is treated securely and in accordance with this Privacy Policy and no transfer of your personal information will take place to an organization or a country unless there are adequate controls in place, including the security of your data and other personal information, and as per applicable data privacy laws."[4]

29. Finally, Academy Mortgage assures its consumers that it "is committed to ensuring that your information is secure. We use commercially reasonable efforts to protect your

[3] Privacy Policy, Academy Mortgage Corporation. https://academymortgage.com/privacy-policy (last visited January 4, 2024).
[4] *Id*.

personal[.]" These protections include "administrative, technical, and physical safeguards."[5]

30. According to the Breach Notice, Academy Mortgage claims that "on March 21, 2023, [it] detected and stopped a network security incident in which an unauthorized third party accessed and disabled some of our systems." Ex. A. Academy Mortgage further admits that an internal investigation revealed that "an unauthorized individual may have accessed certain individual personal information during this incident." Ex. A.

31. In other words, the Data Breach investigation revealed Defendant's cyber and data security systems were completely inadequate and allowed cybercriminals to obtain files containing a treasure trove of thousands of its consumers' highly private information.

32. Through its inadequate security practices, Defendant exposed Plaintiff's and the Class's PII for theft and sale on the dark web.

33. On information and belief, the notorious and aggressive BlackCat, also known as Alphv, ransomware gang took credit for the Data Breach.[6] An incredibly active and successful hacker collective with over 1,000 victims between 2022 and 2023 alone[7], Defendant knew or should have known of the tactics that hackers like BlackCat employ.

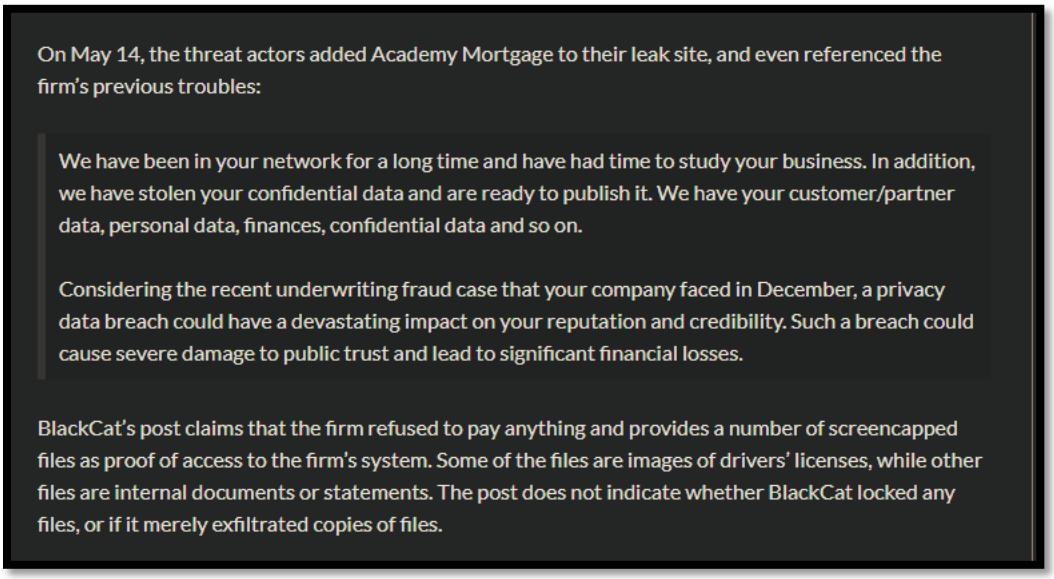
[5] *Id*.
[6] DataBreaches.net, https://www.databreaches.net/only-months-after-dealing-with-one-problem-academy-mortgage-gets-hit-with-a-ransomware-attack/ (last visited January 4, 2024).
[7] StopRansomware, Cybersecurity& Infrastructure Security Agency, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a (last visited January 4, 2024).

34. With the PII secured and stolen by BlackCat, the hackers then purportedly issued a ransom demand to Defendant. However, Defendant have provided no public information on the ransom demand or payment.

35. On information or belief, BlackCat is anticipated to release all stolen information onto the dark web for access, sale, and download following the deadline of the ransom demand to Defendant.[8]

36. Indeed, BlackCat has stated that not only is it going to release all stolen information onto the dark web for sale, but that it has been "in [Defendant's] network for a very long time", reminding Defendant that it has consumers' most sensitive personal data, finances, and confidential data.

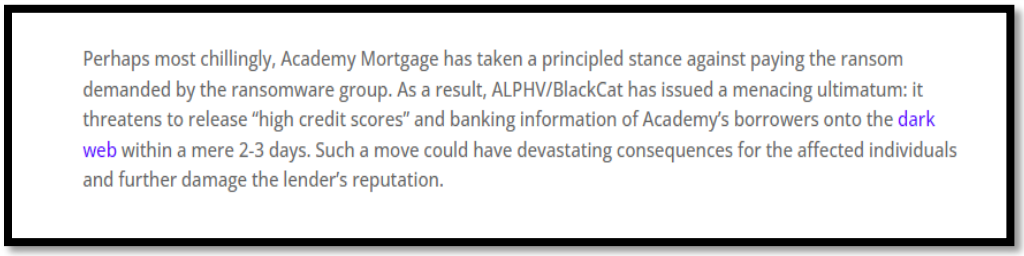
[8] *Id*.



On May 14, the threat actors added Academy Mortgage to their leak site, and even referenced the firm's previous troubles:

> We have been in your network for a long time and have had time to study your business. In addition, we have stolen your confidential data and are ready to publish it. We have your customer/partner data, personal data, finances, confidential data and so on.
>
> Considering the recent underwriting fraud case that your company faced in December, a privacy data breach could have a devastating impact on your reputation and credibility. Such a breach could cause severe damage to public trust and lead to significant financial losses.

BlackCat's post claims that the firm refused to pay anything and provides a number of screencapped files as proof of access to the firm's system. Some of the files are images of drivers' licenses, while other files are internal documents or statements. The post does not indicate whether BlackCat locked any files, or if it merely exfiltrated copies of files.



Perhaps most chillingly, Academy Mortgage has taken a principled stance against paying the ransom demanded by the ransomware group. As a result, ALPHV/BlackCat has issued a menacing ultimatum: it threatens to release "high credit scores" and banking information of Academy's borrowers onto the dark web within a mere 2-3 days. Such a move could have devastating consequences for the affected individuals and further damage the lender's reputation.

37. Despite being directly contacted by BlackCat and being informed that consumers' information would be posted for sale and theft on the dark web, Defendant did not begin notifying Class Members about the Data Breach until December 20, 2023–an appalling nine months after the Data Breach first occurred.

38. Despite its duties to safeguard PII, Defendant, a self-proclaimed leader in its industry, did not in fact follow industry standard practices in securing consumers' PII, as evidenced by the Data Breach.

39. In response to the Data Breach, Academy Mortgage contends that it is or will "take[] steps to bolster our network security" and is "reviewing and altering our policies, procedures, and network security software relating to the security of our systems." Ex. A. Although Defendant fails to expand on what these "steps" and "altercations" are, such actions should have been in place before the Data Breach.

40. Through its Breach Notice, Defendant recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to "place a security freeze", "remain vigilant and monitor your accounts for suspicious or unusual activity" and to "educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself[.]" Ex. A

41. Defendant further recognized their duty to implement reasonable cybersecurity safeguards or policies to protect consumers' PII, promising that, despite the Data Breach demonstrating otherwise, Defendant "value[s] the security of the personal data that we maintain," repeatedly insisting that "[d]ata security is one of our highest priorities" and "[w]e take the privacy of your personal information seriously." Ex. A.

42. Finally, Academy Mortgage also acknowledged through its Breach Notice, its failure to provide adequate information regarding the Data Breach in the Breach notice, acknowledging that "[w]e recognize that you may have questions not addressed in this letter." Ex. A.

43. On information and belief, Academy Mortgage has offered a one year of complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves PII that cannot be changed, such as Social Security numbers.

44. Even with one year of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiff's and Class Members' PII is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

45. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's.

Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

46. On information and belief, Academy Mortgage failed to adequately train its IT and data security employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its consumers' PII. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII.

The Data Breach was a Foreseeable Risk of Which Defendant was on Notice.

47. It is well known that PII, including Social Security numbers, is an invaluable commodity and a frequent target of hackers.

48. In 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[9]

49. In light of recent high profile data breaches, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Academy Mortgage knew or should have known that its electronic records would be targeted by cybercriminals.

50. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

51. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its

[9] Data breaches break record in 2021, CNET (Jan. 24, 2022), https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/ (last accessed September 4, 2023).

own acknowledgment of its duties to keep PII private and secure, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

52. In the years immediately preceding the Data Breach, Defendant knew or should have known that Defendant's computer systems were a target for cybersecurity attacks, including ransomware attacks involving data theft, because warnings were readily available and accessible via the internet.

53. In October 2019, the Federal Bureau of Investigation published online an article titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that, among other things, warned that "[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector."[10]

54. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," that "[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."[11]

55. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms

[10] High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations, FBI, available at https://www.ic3.gov/Media/Y2019/PSA191002 (last accessed September 4, 2023).

[11] Ransomware mentioned in 1,000+ SEC filings over the past year, ZDNet, https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/ (last accessed September 4, 2023).

of extortion."[12]

56. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that (i) ransomware actors were targeting entities such as Defendant, (ii) ransomware gangs were ferociously aggressive in their pursuit of entities such as Defendant, (iii) ransomware gangs were leaking corporate information on dark web portals, and (iv) ransomware tactics included threatening to release stolen data.

57. In light of the information readily available and accessible on the internet before the Data Breach, Defendant, having elected to store the unencrypted PII of thousands of its current and former consumers in an Internet-accessible environment, had reason to be on guard for the exfiltration of the PII and Defendant's type of business had cause to be particularly on guard against such an attack.

58. Before the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiff's and Class Members' PII could be accessed, exfiltrated, and published as the result of a cyberattack. Notably, data breaches are prevalent in today's society therefore making the risk of experiencing a data breach entirely foreseeable to Defendant.

59. Prior to the Data Breach, Defendant knew or should have known that it should have encrypted its consumers' Social Security numbers and other sensitive data elements within the PII to protect against their publication and misuse in the event of a cyberattack.

Plaintiff's Experience and Injuries

60. Plaintiff Lazaro Stern is a former consumer of Defendant and received a Data Breach notice on or around December 23-24, 2023.

61. As a condition of receiving Defendant's services, Plaintiff provided it with his PII,

[12] Ransomware Guide, U.S. CISA, https://www.cisa.gov/stopransomware/ransomware-guide (last accessed September 4, 2023).

including but not limited to his name and Social Security number. Academy Mortgage used that PII to facilitate its services to Plaintiff and required Plaintiff to provide that PII to obtain its mortgage services.

62. Plaintiff provided his PII to Academy Mortgage and trusted that the company would use reasonable measures to protect it according to state and federal law.

63. Defendant deprived Plaintiff of the earliest opportunity to guard himself against the Data Breach's effects by failing to notify him about it for nine months.

64. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's PII for theft by cybercriminals and sale on the dark web.

65. Plaintiff does not recall ever learning that his PII was compromised in a data breach incident, other than the breach at issue in this case.

66. Plaintiff suffered actual injury from the exposure of his PII —which violates his rights to privacy.

67. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

68. As a result of the Data Breach, Plaintiff has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, changing his online account passwords, placing a credit freeze through the three main credit bureaus, and monitoring his credit information.

69. Plaintiff has already spent and will continue to spend considerable time and effort monitoring his accounts to protect himself from identity theft. Plaintiff fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach. Plaintiff has and

is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

70. Plaintiff is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties. This injury was worsened by Defendant's delay in informing Plaintiff and Class Members about the Data Breach.

71. Indeed, following the Data Breach, Plaintiff has experienced an enormous increase in spam calls, up to ten a day, suggesting that his PII is now in the hands of cybercriminals.

72. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

73. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

74. As a result of Academy Mortgage's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. Plaintiff and the class have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in its possession.

75. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

76. The value of Plaintiff's and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

77. Social Security numbers are particularly attractive targets for hackers because they can easily be used to perpetrate identity theft and other highly profitable types of fraud. Moreover, Social Security numbers are difficult to replace, as victims are unable to obtain a new number until the damage is done.

78. It can take victims years to spot identity or PII theft, giving criminals plenty of time to use that information for cash.

79. One such example of criminals using PII for profit is the development of "Fullz" packages.

80. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

81. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and the Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and the Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and members of the Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

82. Defendant disclosed the PII of Plaintiff and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

83. Defendant's failure to properly notify Plaintiff and the Class of the Data Breach

exacerbated Plaintiff's and the Class's injuries by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant failed to adhere to FTC guidelines.

84. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

85. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

86. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

87. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

88. The FTC has brought enforcement actions against businesses for failing to

adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

89. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

90. Several best practices have been identified that—at a minimum—should be implemented by businesses like Defendant. These industry standards include: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

91. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

92. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for

Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

93. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

CLASS ACTION ALLEGATIONS

94. Plaintiff is suing on behalf of himself and the proposed Class ("Class") and state subclass ("Subclass"), defined as follows:

> **Nationwide Class: All individuals residing in the United States whose PII was compromised in Defendant's Data Breach, including all those who received notice of the breach.**
>
> **Florida Subclass: All individuals residing in Florida whose PII was compromised in the Defendant's Data Breach, including all those who received notice of the breach.**

95. Excluded from the Class is Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

96. Plaintiff reserves the right to amend the class definition.

97. Plaintiff and members of the Class satisfy the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23:

a. **Numerosity**. Plaintiff's claim is representative of the proposed Class, consisting of over several thousand individuals, far too many to join in a single action;

b. **Ascertainability**. Class members are readily identifiable from information in Defendant's possession, custody, and control;

c. **Typicality**. Plaintiff's claim is typical of Class member's claims as each

arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. His interest does not conflict with Class members' interests, and Plaintiff has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for all Class members. Indeed, it will be necessary to answer the following questions:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII;

ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendant was negligent in maintaining, protecting, and securing PII;

iv. Whether Defendant breached contract promises to safeguard Plaintiff's and the Class's PII;

v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendant's Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiff's and the Class's injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

f. **Appropriateness**. The likelihood that individual members of the Class will prosecute separate actions is remote due to the time and expense necessary to prosecute an individual case. Plaintiff is not aware of any litigation concerning this controversy already commenced by others who meet the criteria for class membership described above.

g. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

98. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

99. Plaintiff and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their PII, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

100. Defendant owed a duty of care to Plaintiff and Class Members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry standards for data security—would compromise their PII in a data breach. And here, that foreseeable danger came to pass.

101. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if their PII was wrongfully disclosed.

102. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew

or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiff's and Class Members' PII.

103. Defendant owed—to Plaintiff and Class Members—at least the following duties to:

a. exercise reasonable care in handling and using the PII in its care and custody;

b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;

c. promptly detect attempts at unauthorized access;

d. notify Plaintiff and Class Members within a reasonable timeframe of any breach to the security of their PII.

104. Also, Defendant owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiff and Class Members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

105. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII it was no longer required to retain under applicable regulations.

106. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

107. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship

arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a necessary part of employment and/or obtaining medical services from Defendant.

108. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII — whether by malware or otherwise.

109. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff's and Class Members' and the importance of exercising reasonable care in handling it.

110. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

111. Defendant breached these duties as evidenced by the Data Breach.

112. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class Members' PII by:

a. disclosing and providing access to this information to third parties and

b. failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

113. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the PII of Plaintiff and Class Members which actually and proximately caused the Data Breach and Plaintiff's and Class Members' injury.

114. Defendant further breached its duties by failing to provide reasonably timely notice

of the Data Breach to Plaintiff and Class Members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and Class Members' injuries-in-fact.

115. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

116. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

117. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CAUSE OF ACTION
Negligence *per se*
(On Behalf of Plaintiff and the Class)

118. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

119. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

120. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the PII entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of

Defendant's duty to protect Plaintiff's and the Class Members' sensitive PII.

121. Defendant breached its respective duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII.

122. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

123. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

124. But for Defendant's wrongful and negligent breach of its duties owed, Plaintiff and Class Members would not have been injured.

125. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

126. Defendant's violations and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

127. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and

Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*)

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

128. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

129. Plaintiff and the Class delivered their PII to Defendant as part of the process of obtaining services provided by Defendant.

130. Plaintiff and Class Members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members if and when their data had been breached and compromised. Each such contractual relationship imposed on Defendant an implied covenant of good faith and fair dealing by which Defendant was required to perform its obligations and manage Plaintiff's and Class Members' data in a manner which comported with the reasonable expectations of privacy and protection attendant to entrusting such data to Defendant.

131. In providing their PII, Plaintiff and Class Members entered into an implied contract with Defendant, whereby Defendant, in receiving such data, became obligated to reasonably safeguard Plaintiff's and the other Class Members' PII.

132. In delivering their PII to Defendant, Plaintiff and Class Members intended and understood that Defendant would adequately safeguard that data.

133. Plaintiff and the Class Members would not have entrusted their PII to Defendant in the absence of such an implied contract.

134. Defendant accepted possession of Plaintiff's and Class Members' PII.

135. Had Defendant disclosed to Plaintiff and Class Members that Defendant did not have adequate computer systems and security practices to secure consumers' PII, Plaintiff and members of the Class would not have provided their PII to Defendant.

136. Defendant recognized that consumers' PII is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and Class Members.

137. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

138. Defendant breached the implied contract with Plaintiff and Class Members by failing to take reasonable measures to safeguard their data.

139. Defendant breached the implied contract with Plaintiff and Class Members by failing to promptly notify them of the access to and exfiltration of their PII.

140. As a direct and proximate result of the breach of the contractual duties, Plaintiff and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiff and the Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiff's and Class Members' PII; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their PII; (g) the diminution in the value of the services bargained for as Plaintiff and Class Members were deprived of the data protection and security that Defendant promised when Plaintiff and the proposed class entrusted Defendant with their PII; and (h) the continued and substantial risk to Plaintiff's and Class Members' PII, which remains in the Defendant's possession with inadequate measures to protect Plaintiff's and Class Members' PII.

FOURTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of the Plaintiff and the Class)

141. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

142. This claim is plead in the alternative to the breach of implied contractual duty claim.

143. Plaintiff and members of the Class conferred a benefit upon Defendant in the form of services through employment. Defendant also benefited from the receipt of Plaintiff's and the Class's PII, as this was used to facilitate their employment.

144. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff and members of the Class.

145. Under principals of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and the proposed Class's services and their PII because Defendant failed to adequately protect their PII. Plaintiff and the proposed Class would not have provided their PII or worked for Defendant at the payrates they did had they known Defendant would not adequately protect their PII.

146. Defendant should be compelled to disgorge into a common fund to benefit Plaintiff and members of the Class all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged here.

FIFTH CAUSE OF ACTION
Invasion of Privacy
(On Behalf of the Plaintiff and the Class)

147. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

148. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

149. Defendant owed a duty to its consumers, including Plaintiff and the Class, to keep

this information confidential.

150. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff's and Class Members' PII is highly offensive to a reasonable person.

151. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class disclosed their sensitive and confidential information to Defendant as part of their employment, but they did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

152. The Data Breach constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

153. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

154. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

155. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

156. As a proximate result of Defendant's acts and omissions, the PII of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

157. Unless and until enjoined and restrained by order of this Court, Defendant's

wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class because their PII are still maintained by Defendant with its inadequate cybersecurity system and policies.

158. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII of Plaintiff and the Class.

159. In addition to injunctive relief, Plaintiff, on behalf of himself and the other members of the Class, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

SIXTH CAUSE OF ACTION
Violations of the Florida Deceptive and Unfair Trade Practices Act
Fla. Stat. §§ 501.201, *et seq*.
(On Behalf of Plaintiff and the Florida Subclass)

160. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

161. Plaintiff brings this Count on his own behalf and on behalf of the Florida Class (the "Class" for the purposes of this Count).

162. The purpose of the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA") is to "protect the consuming public . . . from those who engage in unfair methods of competition, or unconscionable, deceptive, or unfair acts or practices in the conduct of any trade or commerce."[13]

163. And the Florida Legislature declared that FDUTPA "shall be construed liberally" as to effectuate such purposes.[14]

[13] Fla. Stat. § 501.202.
[14] *Id*.

164. FDUTPA establishes that "[u]nfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful." [15]

165. Plaintiff and Class members all constitute "[c]onsumer[s]" under FDUTPA as they are all "individual[s]."[16]

166. FDUTPA applies to Defendant because Defendant engages in "[t]rade or commerce" such as "advertising, soliciting, providing, offering, or distributing, whether by sale, rental, or otherwise, of any good or service, or any property, whether tangible or intangible, or any other article, commodity, or thing of value, wherever situated."[17]

167. Defendant violated FDUTPA by, *inter alia*:

a. failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class members' PII, which was a direct and proximate cause of the Data Breach;

b. failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*, which was a direct and proximate cause of the Data Breach;

[15] *Id*. at § 501.204.
[16] *Id*. at § 501.203.
[17] *Id*.

d. omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's Class members' PII; and

e. omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq*.

168. Defendant's omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of their PII.

169. Defendant intended to mislead Plaintiff and Class members and induce them to rely on its omissions.

170. Had Defendant disclosed to Plaintiff and Class members that its data systems were not secure—and thus vulnerable to attack—Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Defendant accepted the PII that Plaintiff and Class members entrusted to it while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Class members acted reasonably in relying on Defendant's omissions, the truth of which they could not have discovered through reasonable investigation.

171. Defendant acted intentionally, knowingly, maliciously, and recklessly disregarded Plaintiff's and Class members' rights.

172. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiff and Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including

from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

173. Plaintiff and Class members seek all monetary and non-monetary relief allowed by law, including actual damages, attorneys' fees, and costs.

PRAYER FOR RELIEF

Plaintiff and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing his counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the

evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff hereby demands that this matter be tried before a jury.

DATED this 5th of January, 2024.

MARSHALL OLSON & HULL, PC
BY: /s/ Jason R. Hull
JASON R. HULL

TURKE & STRAUSS, LLP
RAINA C. BORRELLI

ATTORNEYS FOR PLAINTIFFS AND
PROPOSED CLASS COUNSEL